IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE FOLLOWING EMAIL ADDRESSES THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC: (1) ALISONPENNINGTON81@GMAIL.COM; (2) STORYURBANICH87@GMAIL.COM; (3) BILLS9302@GMAIL.COM; (4) CARYNNAWRIGHT85@GMAIL.COM; (5) ANDREWKING33@GMAIL.COM; (6) RAHSHJEEMBENSON69@GMAIL.COM; (7) ANDREWWHITNEY39@GMAIL.COM	Case No. 2:19-mj- 316-JHR **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David J. Pawson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with Homeland Security Investigations (HSI), and have been since 2009. Prior to my tenure with HSI, I was employed as a Border Patrol Agent with the United States Border Patrol from 2005 until 2009. I have participated in numerous criminal investigations, to include matters involving document and benefit fraud and aggravated identity theft. My responsibilities include investigating cases involving persons who have unlawfully obtained and/or used counterfeit and/or altered identification documents such as driver's licenses, resident alien cards, employment authorization documents and passports to fraudulently obtain government benefits or for financial gain. In the course of my law enforcement career, I conducted or participated in numerous other investigations and received training in financial investigations related to frauds, money laundering as well as dark net investigations such as the violations that are the subject of this investigation. I have also assisted in the execution of numerous search and arrest warrants during which evidence of document benefit fraud and identity theft, and other contraband has been found. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

3. This affidavit is based on information learned in the course of my investigation, as well as information communicated to me by witnesses and other law enforcement agents in the course of my investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of federal criminal law, including conspiracy, in violation of 18 U.S.C. § 371, bank fraud in violation of 18 U.S.C. §§ 1344(2) and 2, and aggravated identity theft, in violation of 18 U.S.C. §§ 1028A(1) and 2, have been committed by

Bernard Gardson and Rahshjeem Benson. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On January 15, 2019, a woman by the name of Roza S. Novikov entered a Key Bank branch located at 12 Shapleigh Road in Kittery, Maine and identified herself to Personal Banker Dina Morris as S.H.[1] in order to apply for a loan in the amount of $20,000. In support of the application, Novikov presented a North Carolina driver's license bearing number 82630221 and the name S.H. with a date of birth of xx/xx/xx87, an Army National Guard paystub also in the name of S.H. (with a purported address in South Portland, Maine), and social security number xxx-xx-xx48 which was written on a piece of paper. During the loan application process, Novikov signed a form entitled "KeyBank Authorization to Release Information" which listed the following information: Automated Credit Application Processing System (ACAPS) Number 190151254320C, which in turn identified the borrower as "S.H.," with a mailing address in Old Fort, North Carolina. This resulted in the credit history of the true S.H. being checked without actual authorization. Novikov also provided an email address when she completed the loan application – storyurbanich87@gmail.com.

[1] I am using initials throughout in order to protect the identity of the victim in this case, as well as redacted versions of the victim's personal identifiers.

7. Using the alias of S.H., Novikov claimed during the loan application process that her father had been diagnosed with pancreatic cancer three years prior and that she needed to move her husband and two children from North Carolina to Maine to care for her dying father. Novikov specified that she needed the loan proceeds for funeral expenses as well as living expenses. Key Bank staff felt the situation was suspicious and notified the Kittery, Maine Police. They also informed the police that they had observed "S.H." cross the street and get into the passenger side of a black Chevrolet Suburban that was parked in the parking lot of a Rite-Aid pharmacy.

8. Kittery Maine Police Detective Brian Cummers contacted law enforcement officers in North Carolina and determined that the driver's license number displayed on the license was not on file with the state of North Carolina. Detective Cummer then attempted to contact the Army National Guard office in South Portland, Maine, using the telephone number displayed on the paystub and discovered that the telephone number was no longer in service. Detective Cummers ultimately spoke with Maine Army National Guard Sergeant Brown who explained that the office address listed on the paystub had been closed for approximately one year. Sergeant Brown also told Detective Cummers that he did not recognized the name S.H. as a member of the Army National Guard. Sergeant Brown forwarded a copy of his personal paystub for comparison purposes to Detective Cummers. Detective Cummers noted that the formats and information displayed were different from those that appeared on the paystub Novikov had presented. Detective Cummers also noted that the actual National Guard paystubs do not display the employer's name, address or telephone number on them.

9. On January 16, 2019, Kittery Patrol Officer Robert Byrnes went to the Rite-Aid pharmacy and learned that they had cameras on the outside of the building. Officer Byrnes

reviewed the camera footage and noted that a black Suburban had pulled into the parking lot on January 15, 2019, at approximately 11:25 a.m. He also observed that a woman (later identified as Roza Novikov) got out of the passenger side at 11:37 a.m. and walked across the street into the bank. At approximately 12:10 p.m., Novikov returned to the Suburban and sat there until approximately 12:20 p.m.

10. On January 17, 2019, Novikov returned to the Key Bank branch in Kittery in order to finalize her loan. Bank employees alerted Detective Cummers about Novikov's presence at the branch and he responded to investigate, along with Officer Byrnes and another member of the Kittery Police department. Officer Byrnes was the first on the scene, and observed a dark colored Suburban bearing Massachusetts license plate number 8ZF525 parked in the same spot in the Rite-Aid parking lot as on January 15, 2019. Officer Byrnes approached the driver's side door of the Suburban and observed two black males sitting in the front seat. Officer Byrnes tapped on the window and engaged the driver, who later identified himself as "A.W." and provided a New York driver's license in the name of A.W., which bore the driver's photograph. A.W. denied that he had been to Maine previously, and claimed not to know Novikov. When Detective Cummers arrived, he met with Novikov inside the Key Bank branch, who then presented him with yet another driver's license, this time bearing the name C.W. and indicating it had been issued in South Carolina. Eventually, the man claiming to be "A.W.", Novikov and the passenger who was in the vehicle with "A.W." (later identified as Giovanni Williams) were arrested that day by the Kittery Police. While inventorying the contents of "A.W."'s wallet, Detective Cummers noticed a credit card in the name of Rahshjeem Benson. Detective Cummers returned to the booking room and asked "A.W." if he was in fact Rahshjeem Benson. Benson continued to claim that he was "A.W."

11. On January 18, 2019, I met with and interviewed Novikov after first providing her with her Miranda warnings. Novikov told me that she met an individual she called "6" in Boston, Massachusetts, and that "6" had recruited her to apply for bank loans in the name of real people, using fraudulent identification documents. She told me that "6" was the tall black male who had been driving the Suburban and claiming to be A.W. Novikov also told me that an individual named "Geo" or "BG3" was the person behind the scam, and was the one who purchased the personal information of real people on the internet who had excellent credit scores. According to Novikov, "Geo" would then arrange to have bogus driver's licenses in the name of the stolen identities made by a contact in Las Vegas, Nevada. "Geo" also provided Novikov with other supporting documents (such as the bogus National Guard paystub) as evidence of identity to use when she applied for personal loans in the names of the individuals whose personal identifying information "Geo" had acquired.

12. Novikov eventually waived indictment, pled guilty and agreed to cooperate with the ongoing investigation. During the course of that investigation, I determined that "Geo" was in fact Bernard Gadson, and "6" was in fact Rahshjeem Benson. On June 20, 2019, a federal grand jury returned an indictment charging Gadson and Benson with attempted bank fraud, in violation of 18 U.S.C. §§ 1344(2) and 2, aiding and abetting aggravated identity theft, in violation of 18 U.S.C. §§ 1028A(1) and 2, and conspiracy, in violation of 18 U.S.C. § 371. The case is captioned *United States v. Bernard Gadson and Rahshjeem Benson*, Criminal No. 2:19-cr-00122-DBH, and is currently set for trial on November 13, 2019.

13. During the course of my investigation, I was able to determine that Novikov, at the direction of Benson and Gadson, had applied for personal loans at banks and credit unions throughout New England in the name of at least four different women, during the period from

approximately December 26, 2018, through the date of her arrest in January, 2019: (1) S.H.; (2) C.W.; (3) S.B.; and (4) A.P. Each time that she applied for loan, Novikov provided an email address for each of these individuals. On October 18, 2019, during the course of debriefing Novikov, I learned that those email addresses were actually real gmail addresses that Gadson had created for the sole purpose of facilitating the bank fraud scheme. According to Novikov, Gadson would create gmail accounts in the name of the victims and then provide her with the password for each account, so that both she and Gadson could use the gmail address to communicate with the victim financial institutions during the course of the fraud. The sole purpose of creating these gmail accounts was to be able to provide documents and other information requested by banks and credit unions in connection with the fraudulent loan applications.

14. I have reviewed loan applications submitted by Novikov during the period of the conspiracy in the names of the above-referenced victims, and determined that she provided the following email addresses in connection with the scheme (one for each victim whose identity had been stolen): carynnawright85@gmail.com; alisonpennington81@gmail.com; storyurbanich87@gmail.com; and bills9302@gmail.com.

15. During the course of the investigation, I learned that Rahshjeem Benson had rented the Chevy Suburban he was operating on the day of his arrest in the name of A.W. from Enterprise Car Rental in East Boston, on January 3, 2019. When Benson rented the Suburban from Enterprise, he provided the following email address: andrewwhitney39@gmail.com. I also obtained records during the course of the investigation documenting the fact that during the month of January 2019, Benson purchased two airline tickets from American Airlines using the name and personal identifiers of A.W. In connection with one purchase, Benson used the email

address of rahshjeembenson69@gmail.com, and in connection with the other purchase, Benson used the email address of andrewking33@gmail.com.

BACKGROUND CONCERNING EMAIL

16. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

18. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

21. Based on the forgoing, I request that the Court issue the proposed search warrant.

22. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant

by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

David J. Pawson, Special Agent
Homeland Security Investigations

Sworn to and subscribed before me on this 21st day of October, 2019.

John H. Rich III
United State Magistrate Judge